2014-06-01

Open Enterprise Information System (OEIS) Procurement Best Practices

Gunderson, C.R.

OPEN ENTERPRISE INFORMATION SYSTEM (OEIS) PROCUREMENT BEST PRACTICES

By C. R. Gunderson
Naval Postgraduate School Department of Information Science

On behalf of Office of the Undersecretary of Defense for Intelligence (OUSD (I))

1 June 2014

Table of Contents

Background

Government policy has emphasized use of "enterprise," "open," and "collaborative" approaches to building information systems for many years. Per myriad watchdog reports, results have been overwhelmingly unsatisfactory. Studies and watchdog reports document many failures and relatively few successes. Nevertheless, both successes and failures point to some best practices, and practices to avoid, as summarized below. The Value Assurance Framework (VAF) developed by NPS on behalf of OUSD (I) provides tools for implementing these best practices.

Observations

Open system development is fundamentally different than traditional waterfall development. Government PMs are not typically trained in appropriate open system acquisition practices. Likewise government contractors are typically not expert in open system development.

The overarching VAF contracting strategy is based on the fundamental truths that "you get what you measure" and "you get what you pay for." VAF asserts that enterprises should write contracts that measure and pay for [[Value] equals [Utility-per-Cost] divided by [Time it Takes to Deliver Utility]]. Accordingly VAF solicitation,

source selection, and contract incentives are based on objective V&V as described above. That is, vendors must use VAF tools to verify that their lifecycle system and process performance is consistent with the contractually mandated exponential improvement predicted by Moore's Law. Integrators must then apply VAF tools to validate that verified exponential system and process improvements lead to exponential improvement in targeted mission outcomes, i.e. RoI.

In developing open systems, the most important requirements, and the greatest risk, is associated with carefully scoping, defining and assuring interoperability. Both "operational Interoperability", i.e. ability to usefully share networked data and resources in run time, and "engineering interoperability", i.e. ability to plug-and-play off-the-shelf hardware and software, are critical.

Information Assurance (IA) is an element of both operational and engineering interoperability. Traditional approaches to IA and Certification and Accreditation (C&A) do not adequately address "need-to-share" and severely inhibit ability to achieve the desired level of interoperability.

The objective of open system development is to leverage agile plug-and-play development to improve utility-per-capability, speed-to-capability, and lifecycle cost-per-capability. Success requires carefully defining and testing against objective metrics for each of these objectives.

In the early 1990's the Secretary of Defense recognized that (1) software was becoming an increasingly important aspects of military systems; and (2) that success in acquiring software would require new paradigms that emphasize flexibility and agility. In response, the Office of the Secretary of Defense (OSD) issued Military Standard number 498 (MILSTD 498.) MILSTD 498 provides tailorable templates called Data Item Descriptions (DID). These templates translate laymen's descriptions of requirements associated with software-intensive projects into clear technical descriptions of contract deliverables.

OSD, expecting that better commercial standards would quickly evolve, believed that MILSTD 498 would be become obsolete and stopped maintaining it. However, no commercial standard for best practices across the disciplines of project management, software-intensive systems engineering, and contracting, ever emerged. Fortunately, MILSTD 498 – even though it is not maintained -- remains an excellent tool for crafting procurement artifacts aligned with OEIS.

According to the Defense Acquisition University (DAU) a Systems Engineering Plan (SEP) helps "…Program Managers develop, communicate, and manage the overall systems engineering (SE) approach that guides all technical activities of the program. A SEP documents key technical risks, processes, resources, metrics, SE products, and completed and scheduled SE activities…the Government SEP should accompany the request for proposal (RFP) as guidance to the offerors. The developer's systems engineering management plan (SEMP), which is the contractor-

developed plan … should be consistent with the Government SEP…." Despite this clear guidance, frequently the government either does not provide a SEP with its solicitation, or provides a traditional SEP that is not well aligned with OEIS best practices.

Existence of excellent, tailorable, tools such as MILSTD 498 and SEP notwithstanding, government OEIS solicitations and contract award processes tend to reuse legacy boilerplate language and process that is not appropriate for developing modern OEIS.

Recommendations

Use MILSTD 498 , and/or DIDS developed by successful projects, as a guide for tailoring software-intensive contract deliverables.

Identify targeted cost, performance and schedule efficiencies enabled by operational and engineering interoperability. Likewise, identify associated risks that have historically precluded achieving these objectives. Develop a risk/reward optimization strategy and acquisition strategy including for COTS-friendly, OEIS accordingly. (See Appendix (A) for example.)

As with architecting and engineering, VAF suggests adapting existing contracting tools and best practices, rather than inventing new ones out of whole cloth, whenever possible. With that in mind, VAF suggests using the Acquisition.Gov Seven Steps to Performance Based Acquisition (PBA) as a means to build value assurance into contract artifacts. (Acquisition.Gov, 2009) Indeed, the Seven Steps provide superb guidance as to how to frame a performance-based acquisition. VAF complements the Seven Steps by providing more specific implementation tools appropriate for Open EIS., and equating "performance" with "assuring value, i.e. RoI" in the case of Open EIS.
(See Appendix (B) for example.)

Develop validated and verifiable MOE and MOP, associated threshold and objective values, and test methods. Include these in the PWS and RFP. (See Appendix (C) for example.)

Make IA a critical consideration. Build security in from the ground up, but with need-to-share and need-to-protect carefully balanced. Require contractor to address this concern explicitly in RFP. (See Appendix (D) for example.)

Develop a government Systems Engineering Plan (SEP) based on the considerations explained above. Use the OSD SEP Outline as a guide, but streamline and tailor extensively as appropriate for OEIS. The tailored SEP should include high-level drawings of target architecture, schedule, risk strategy and test strategy…all aligned with open systems approaches. Include the SEP in the RFP. The SEP should address IA explicitly. The SEP should explain boundary conditions such as requirements,

any mandated standards, enforceable policies, budgets, timelines, and especially specially targeted outcomes in explicit, objective, engineering terms. It should not constrain vendor innovation in the detail of execution, on the contrary!

Develop source selection criteria based on contractor's credibility with respect to assuring engineering and operational interoperability, per SEP.

Appendices: (A) Sample OEIS Acquisition Strategy excerpts
(B) Sample OEIS Project Work Statement (PWS) excerpts
(C) Sample OEIS Measures of Performance and Effectiveness
(D) Sample OEIS Information Assurance (IA) Plan

Appendix (A): Sample OEIS Acquisition Strategy Excerpts

PROGRAM: Counter-Narco Terrorism Program Office (CNTPO).

PROJECT: Counter Trafficking Information Sharing System-of-Systems (CTIS3) Life Cycle Improvement (LCI) Multi-Agency Collaboration Environment (MACE)

DESCRIPTION OF PROGRAM: … data sharing and analytical challenges by leveraging the lessons learned during counter asymmetric operations in U.S. Central Command (USCENTCOM) operating directives. Presently there are insufficient Intellegence Surveillance Reconnaissance (ISR) capabilities, lack of efficient Processing, Exploitation and Dissemination (PED) capabilities in joint, multi-agency, and multi-national construct which limits the capacity to conduct warfare planning. This also limits the ability to detect, identify, locate, and track high-value targets, for both Counter-Terrorism (CT) and Counter-Narcotics (CN) missions. Specifically, for CN, initiated in early CY13, lack of collection and information sharing in Afghanistan limited the mission effectiveness and force protection for the Afghan drug enforcement police as they prosecute Afghan drug traffickers.

The proposed acquisition is for incremental lifecycle improvement of CTIS3 capability … to provide Intelligence, Surveillance and Reconnaissance (ISR) and Detection and Monitoring (DM) capability for the Drug Enforcement Administration (DEA) that would interoperate with, and support DoD systems and missions. Interoperability with existing DoD and DEA hardware and software is critical to successful CTIS3 missions.

…snip…

1. Requirement

a. Continuously evolving requirements for the CTIS3 are derived from the "living" CONOPS documentation provided as Appendix A to this acquisition strategy. Appendix B and Appendix C explain how CTIS3 will apply tightly coupled, objective, leading and lagging metrics to clearly articulated goals, objectives, and associated risks to assure that targed value is delivered. Generally desired outcomes to be satisfied are as follows:

(1) Improve the ability of the Drug Enforcement Administration's CTIS3 to collect (through multiple means), process, and share information in collaboration with DoD, securely, across stakeholder information domains.

(2) Achieve enhanced speed-to-capability by leveraging Open System Architecture (OSA) to rapidly test, evaluate, and integrate best available Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) Information Technology (IT).

(3) Reduce lifecycle costs of CTIS3 and interoperating systems by leveraging OSA to re-use best available GOTS and COTS IT.

(4) Enhance security and privacy of information shared with/by CTIS3 through high assurance, dynamic, policy-based, virtual techniques.

b. The CTIS3 LCI project will use performance-based methods in accordance with Federal Acquisition Regulation (FAR) Subpart 37.6 Service Acquisition.

c. The government will use threshold and objective critieria keyed to objective Measures of Effectiveness (MOE), Measures of Performance (MOP), and Measures of Suitabilility (MOS) to define the success of this acquisition in terms of cost, performance, and schedule. These measures will address operational, system, process, and financial performance according to the following high level strategy:

(1) Improve the ability of the DEA's 's CTIS3 to collect, process, and share information in collaboration with DoD, securely, across stakeholder information domains.

Threshold: Operational test validates that new capability enhances specified MOE, MOS, and/or MOP compared to specified legacy benchmark.
Objective: Operational test validates that new capability enhances specified MOE, MOS, and/or MOP by at least ten percent compared to specified legacy benchmark.

Threshold: Capabilities delivered under CTIS3 LCI project deliver data and value-added products to DoD systems.
Objective: Capabiltities delivered under CTIS3 LCI project receive data and value-added products from DoD systems.

(2) Achieve enhanced speed-to-capability by leveraging OSA to rapidly test, evaluate, and integrate best available COTS and GOTS IT.

Threshold: new capability identified, integrated, tested, and certified within twelve months of task start date
Objective: new capability identified, integrated, tested, and certified within six months of task start date

(3) Reduce lifecycle costs of CTIS3 and interoperating systems by leveraging OSA, specifically Product Line Architecture (PLA) to re-use best available GOTS and COTS IT.

Threshold: Govermnent-approved lifecycle cost model of new capability predicts enhanced capability-per-cost across specified lifecyle

Objective: Government-approved lifecycle cost model of new capability predicts at least 10% capability-per-cost improvement across specified lifecyle

(4) Enhance security and privacy of information shared with/by CTIS3 through high assurance, dynamic, policy-based, virtual techniques.

Threshold: New data and/or network resources certified and accredited (C&A) at Protection Level 4-equivalent, as sharable, low-to-high, across one security level, in near realtime, via specified Internet Protocol (IP) networks. Objective: New data and/or network resources C&A'd at Protection Level 4-equivalent, as sharable, high-to-low, across one security level, in near realtime, via specified IP networks.

...snip....

f. The challenges for this acquisition concern overcoming historical government acquisition process difficulties in achieving interoperability across system boundaries (including security issues) and fielding emerging technology fast enough to harvest its competitive advantage. Accordingly this acquisition strategy identifies both of those factors as principle risks and implements appropriate methods, tools, and incentives to overcome them.

…snip…

j. DoD creates this acquisition pathway for information collecting, processing, and sharing. IT facilitates the successful integration of these objectives as defined in the Clinger Cohen Act (CCA) 40 USC Chapter 11. CCA mandates that government should apply commercial best practices, including especially OSA, in order to harvest the value of COTS IT capabilities. The CNTPO has partnered with the Multi-Agency Collaboration Environment (MACE) research initiative . The MACE research initiative is a government/industry partnership sponsored by the Under Secretary of Defense for Intelligence (USD-I)) and Deputy Assistant Secretary of Defense, Counter Narcotics & Global Threats (DASD CN&GT) to develop better approaches to acquiring Enterprise Information Systems (EIS) such as CTIS3. MACE aims specifically to capture commercial best practices for interoperability and agile development within constrainsts of government acquisition process. Hence, CTIS3 LCI project goals, objectives, measures, risk management strategy, and contract award critiera all specifically focus on achieving measurably better acquisition value-per-cost-per-time by consuming best-of-breed COTS IT in rapid development spirals.

2. <u>Risk Management</u>

Appendix C: CTIS3 Risk/Reward Optimization Strategy, describes the CTIS3 LCI risk management methodology in detail. This CTIS3 strategy includes the notion that risk must be evaluated in context with targeted reward. The contractor shall plan and objectively track both progress toward achieving "reward," and mitigating associated risk. The CTIS3 T&E plan shall specifically support the CTIS3 risk management plan.

a. **Cost risk is MEDIUM**: Chief risk to cost is that lifecycle maintenance costs across the fleet of proprietary DEA airborne ISR systems are not sustainable. Chief reward is substantially reduced life cycle costs across the enterprise achievable by standardizing the family of DEA ISR systems via the Open Standard Approach (OSA) being piloted by the CTIS3 LCI acquisition.

CTIS3 risk/reward optimization strategy for cost includes: a) designing the CTIS3 OSA according to COTS best practices for OSA so that best available COTS and GOTS components, with predicable lifecycle costs, can be readily consumed; b) using credibly modeled lifecycle costs as a key performance metric and downselect criteria.

b. **Schedule risk is HIGH** : Chief risk to schedule is that the acquisition process will not field rapidly evolving COTS technology fast enough to harvest the competitive advantage. Chief reward comes from best available COTS IT that is quickly integrated into the CTIS3 and will provide an asymmetric information processing advantage over the adversary.

CTIS3 risk/reward optimization strategy for schedule includes: a) making acquisition process efficiency (measured in terms of calendar time required to down-select or develop, bundle, test, and certify incremental capability upgrades) a key performance metric; b) using commercial best practices for PLA to rapidly integrate best available COTS/GOTS components.

c. **Performance risk is HIGH**: Chief risk to performance is that the CTIS3 will not be interoperate adequately with DoD and other stakeholder systems. Chief rewards are reduced acquisition costs/schedule associated with reusing system components and enhanced operational effectiveness associated with focused access to more networked data and resources.

CTIS3 risk/reward optimization strategy for performance includes: defining run-time and build-time interoperability objectively, and including build-time and run-time interoperability as key performance metric; defining need-to-share security policies in addition to need-to-protect security policies.

d.Technical risk is HIGH: Chief technical risk is closely related to chief performance risk, i.e. that CTIS3 will not adequately interoperate with other information system. One chief technical risk is potential failure to adequately define, and strictly comply with

open standard interfaces associated with PLA. Government acquisitions typically struggle with this issue.

Another chief technical risk is that by emphasizing use of generic open standard components, specialized performance requirements will not be adequately addressed. Chief rewards are the same as associated with performance risk, namely reduced acquisition costs/schedule associated with reusing system components and enhanced operational effectiveness associated with focused access to more networked data and resources.

CTIS3 risk/reward optimization strategy for technical concerns includes: using best commercial practices for specifying and verifying functions and interfaces within PLA; making compliance with interface specifications a key performance metric; working with Joint Interoperabiltiy Test Command (JITC) throughout capability lifecycle to assure compliance with best practices for interoperability engineering; working with all relevant Designated Approval Authorities (DAA) throughout capability lifecycle to assure that Information Assurance Certification and Accreditation arguments balance the need-to-protect with the need-to-share data and resources.

3. <u>Competition</u>

…snip….

b. Market Research - … applied the following techniques, between July and November 2013, to identify qualified performers for CTIS3 lifecycle improvement:

Extensive dialog with not-for-profit industrial associations such as the Armed Forces Communications and Electronics Association and the National Defense Industrial Association, including especially deep dives via the new "Plug Fest" methodology for evaluating interoperability.

Internet word search and follow up with various vendors

Dialog with government leaders within various programs and projects with similar objectives

Past experience with similar contracts and programs

Reach back to and discussion with specialists and researchers at the Naval Postgraduate School

Discussions with current mission partners, to include DEA, US CENTCOM, US SOCCOM, Joint Interagency Task Force (JIATF) South, JIATF-West, El Paso Intelligence Center (EPIC), Joint Task Force, North (JTF-N).

Specifically, this market survey explored the following seven expertise requirements:

1. Open System Architecture
2. Airborne ISR
3. PED systems
4. End to End test and certification of data sharing systems
5. Military and commercial communications via software defined radios
6. Integration of data (i.e., critical infrastructure data) into an enterprise framework
7. Information Assurance, Cross Domain Solutions and associated Certification and Accreditation C&A via logical separation

…snip…

4. Metrics

The contractor will propose, and/or the government will provide/approve objective operational level, system level, process efficiency, and financial MOE, MOS, and MOP. The government wil furnish guidance by providing the current version of Appendix B: CTIS3 Value Assurance Framework to the contractor.

Operational level measures include Probability of Detection (P_D) and/or Probability of Intercept (P_I) or other similar quantifiable indicators of mission effectiveness approved by government operational customers.

System level measures include reliability, availability, message latency, protection level, camera resolution, field of view, standard compliance, or other quantifiable indicators of system effectiveness approved by government technical authority.

Process level measures include sequential calendar time required to perform activities such as inventing new capabilities, discovering and evaluating existing capabilities, bundling existing capabilities, testing, certifying, performing overhead functions, or other quantifiable measure of availability of acquisition process efficiency approved by government technical authority.

Financial measures shall objectively quantify expected lifecycle costs as predicted by standard commercial and/or government models approved by the government.

Contractor shall propose, and government will approve baseline values, threshold and objective evaluation criteria, and acceptable approaches to Validation and Verification (V&V).

Contractor shall provide, and government will approve Test and Evaluation (T&E) plans that explain the V&V strategy and provide schedule of T&E and other V&V events.

Contractor shall explicitly include T&E strategy and schedule as a central component of a risk tracking and mitigation strategy.
The contractor will propose the government will approve models and measurement techniques to be applied in test and/other V&V events.

The contractor shall apply any government provided historical baseline values, or determine baseline values prior to V&V using the same modeling and/or measurement techniques as to be used in the test or other V&V technique.

Government intends to leverage best available commercial off the shelf (COTS) Information Technology (IT) components. Wherever appropriate, contractor shall equate CTIS3 system-level performance standards and measures to commercial best practice.

…snip….

Appendix (B): Sample OEIS Project Work Statement (PWS) excerpts

PART 1

GENERAL INFORMATION

…snip…

1.2 Background: The illegal narcotics trade is used as a source of funding and support for many terrorist activities worldwide. Part of the Department of Defense (DoD) Counternarcotics (CN) mission includes targeting worldwide terrorist groups that use narcotics trafficking to support these activities. DoD will use its resources in regions where terrorists benefit from illicit drug revenue or use drug smuggling systems. DoD supports government agencies and departments, as well as partner nations' anti-trafficking and counter threat finance efforts worldwide. In particular, per the National Defense Authorization Act (NDAA) FY 1991, section 1104 (reference 5.p), the Office of the Secretary of Defense (OSD) supports the ability of the Drug Enforcement Agency (DEA) systems to interoperate with DoD systems.

..snip…

The DASD CN&GT investment strategy for their programs aims to enable cross-department collaboration by incentivizing and supporting effective information collection and sharing of time sensitive data and information. Counter trafficking enterprise information systems must support rapidly evolving missions, mission partners, areas of operations, and concept of operations. These systems must heavily leverage and not replicate information technology infrastructure and/or tools provided by other government organizations. In order to accomplish this mission, CNTPO applies lessons learned and expertise in Open System Architecture (OSA) to support real world multi-organizational collaborative operations.

The CTIS SoS is composed of two subsystems: (i) Aircraft Mission Payload (AMP), i.e., an embedded Internet Protocol (IP) fiber network, open standard interfaces, and "plug-and-play" communications and surveillance sensors, emitters, and processors designed to support airborne Intelligence Surveillance and Reconnaissance (ISR) and Detection and Monitoring (DM); (ii) Portable Scalable Processing, Exploitation, and Dissemination System (PS-PEDS), i.e., various Commercial off the Shelf (COTS) Information Technology (IT) devices loaded with COTS and Government off-the-shelf (GOTS) software appropriate for interfacing with AMP capabilities via IP networks. AMP and PS-PEDS are designed as open standard product lines meant to evolve and extend across the Counter Trafficking (CT) community as technology and the CT mission evolve.

…snip….

Accordingly, the CT IS SoS life cycle concept will include evolving communications adapter kits. This capability may be provided as a part of the PS-PEDS, AMP, and/or as one or more ancillary kits, depending on specific mission needs. For example, PS-PEDS adapter kits can include software interfaces that allow IP data sharing across any military or commercial standard communications transport medium. If no existing Cross Domain Solution (CDS) is available on at a classified ground site, a small tactical Virtual, Real-time, Dynamic-policy-based CDS (VRDC) can be procured as part of the PS-PEDS adapter kit.

Similarly, the AMP and PS-PEDS product lines are designed with open standards to support rapidly swapping or upgrading the off-the-shelf software. AMP is designed to easily transition to Unmanned Aerial Vehicles, or fixed ground sensor networks. Further, a lightweight variant of PS-PEDS can be installed on the smallest of IT devices to include tablets and Smart Phones, especially as the technology associated with those devices inevitably improves. These PS-PEDS variants can and will evolve to interface with CT community data centers, including increasingly CT data and service "clouds."

…snip….

1.3 Objectives: The objectives of this effort are as follows:

1.3.1. Rapidly evolve and improve the ability of the CT IS SoS to collect, process, and share information in collaboration with DoD, securely, across stakeholder information domains.

1.3.2. Achieve enhanced speed-to-capability by leveraging Open System Architecture (OSA) to rapidly test, evaluate, and integrate best available COTS and GOTS IT.

1.3.3. Reduce lifecycle costs of CT IS SoS and interoperating systems by leveraging re-use of best available GOTS and COTS IT.

1.3.4. Enhance security and privacy of information shared with/by CT IS SoS through integration of high assurance, dynamic, policy-based, virtual techniques.

1.4 Scope: This PWS defines the effort required to design, build, test, certify, enhance, improve, deploy and maintain the CT IS SoS via OSA in general, and via enhancement to the previously developed PS-PEDS and AMP subsystems in particular.

All systems shall be designed to support rapidly evolving missions, mission partners, areas of operation and Concepts of Operations (CONOPS). Systems shall be designed to intercept rapidly evolving technological tools. An OSA shall be used with rapid adaptive engineering and acquisition techniques. All hardware and software

developed for CT IS SoS will have plug-and-play functionality with existing hardware and software.

Test and engineering support is required for both engineering evaluations (informal testing) and formal testing. Engineering evaluations are significantly smaller in scope than formal testing. Test support shall include test planning, test execution and post-test analysis. Engineering evaluation contractor support services shall include engineering evaluation planning, execution and post-engineering evaluation analysis.

1.4.1 Deliverables: Engineering evaluation deliverables shall include engineering evaluation plans, procedures, and reports. An engineering evaluation will typically run two weeks and is narrowly focused on specific capability, subsystem or system.

1.4.2 Interoperability: Interoperability with existing DoD and DEA hardware and software is critical to successful GD missions. Interoperability is the critical performance objective in the CT IS SoS. Interoperability is defined as:

> **Build-time interoperability** = Component-level off-the-shelf functionality, i.e., capability configures out-of-the box, is readily certifiable, is readily consumed from a convenient catalog and procurement vehicle, and comes with well-specified life-cycle support model at known costs.
>
> **Run-time interoperability** = Meaning of the data is shared; the content of the information exchange requests are unambiguously defined; and delivery of critical information to critical decision nodes is assured per a specified information availability metric.

…snip….

1.6.7 Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

….snip….

PART 4

SPECIFIC TASKS

4. SPECIFIC TASKS: The following paragraphs describe specific categories of tasks to be performed under this contract. Task Orders will include specific standards and deliverables.

4.1. Basic Services: In execution of this contract, the Contractor shall provide the following:

4.1.1. The contractor shall study the reference material in part 6 and apply as appropriate in the performance of all tasks.

4.1.2. The contractor shall apply commercial best practices for rapid, adaptive, engineering of open system architecture as defined by the Defense Acquisition University in order to improve measured mission outcomes, speed-to-capability, and cost-per-capability delivered. These architectures are as defined in Federal Standard 1037C of 7 Aug 1996 and discussed in section E1.1.27 of DODD 5000.1 of 20 Nov 2007.

4.1.3. The contractor shall establish processes for frequent interaction with and feedback with both the operational customer community and the acquisition community.

4.1.4. The contractor shall apply methods such as described in MILSTD 498 to propose tailoring of Data Item Descriptions (DID) associated with each specific task deliverable. These DIDS will deliberately tailor the documentation process while maintaining sufficient rigor and repeatability as required to satisfy the intent of Defense Acquisition Guidebook of 28 Jun 2013, DAU OSA Contract Guidebook v1.1 of Jun 2013, , INCOSE SEBoK, and PMIBoK.

4.1.5. The contractor shall propose performance tailored metrics, information assurance approaches, and risk management strategies that optimize value achieved though sharing information among all operational participants as well as among acquisition participants.

4.1.6. The contractor shall propose methods to streamline capturing and sharing government-developed designs, processes, and software such as use of open repositories and open licenses for implementation and repeatability.

4.2. Portable Scalable Processing Exploitation and Dissemination System (PS-PEDS)

4.2.1. PS-PEDS Host Environment: The contractor shall integrate open standard PED software and/hardware according to the GFI PS-PEDS reference architecture (Appendix 1), such that identified operational outcomes are measurably improved, lifecycle costs and methods are identified and documented, as discussed in

paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.2.2. PS-PEDS Communications Kit: The contractor shall select, provide, and/or integrate communications equipment within GD ground stations according to the GFI PS-PEDS reference architecture, to improve and enhance information and data sharing among operational users such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.3. Aircraft Mission Payload (AMP)

4.3.1. AMP Sensor Integration: The contractor shall select, provide, and/or integrate sensors within GD and system airborne platforms according to the GFI AMP reference architecture (Appendix 2), such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented, as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.3.2. AMP Communications System Integration: The contractor shall select, provide, and/or integrate communications equipment such as antennae and radio processors within CT airborne platforms according to the GFI AMP reference architecture, such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented, as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.4.Virtual Dynamic Real-time Cross-Domain Services (VDRC): The contractor shall select, provide, fabricate, and/or integrate VDRC according to GFI AMP and/or PS-PEDS reference architecture, such that GFI need-to-share policy is implemented at PL-4 equivalent assurance, via the requisite communications network. This implementation will make use of a hypervisor and the architecture will follow the guidelines of the trusted Computing Base, such as described by NSA 2014. Task order will provide specific performance standards and deliverables.

4.5. Test and Evaluation (T&E): The contractor shall perform T&E tasks associated with any or all deliverables under this contract, including early development of a Test Plan and identification of resources necessary to complete the assigned task, reports, consistent with operational, system, and process level performance statements specified in task order.

4.6. Certification and Accreditation (C&A): The contractor shall perform evidence collection and documentation tasks necessary to support C&A of any or all deliverables under this contract. Task order will provide specific performance standards and deliverables.

...snip.....

PART 5

APPLICABLE PUBLICATIONS

5. APPLICABLE PUBLICATIONS: The following publications are applicable to the work described in this PWS.

a. INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

b. DOD DIRECTIVE 8320.02: DATASHARINGINANET-CENTRICDEPARTMENT OF DEFENSE, 2007

c. DOD DIR 8320.02G: GUIDANCE FOR IMPLEMENTING NET-CENTRIC DATA SHARING, APR 2006

d. CJCSI 6212.01F: NETREADY KEYPERFORMANCE PARAMETER (NRKPP), 21 MARCH 2012

e. DOD COUNTERNARCOTICS & GLOBAL THREATS STRATEGY

f. GD CONOPS, 22 NOV 2010

g. GD CONOPS DRAFT ANNEX, 14 JAN 2014

h. MEMORANDUM FOR THE RECORD: MISSION NEED STATEMENT FOR CROSS DOMAIN SOLUTIONS (CDS) FOR GLBAL DISCOVERY INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) PROCESSING, EXPLOITATION AND DISSEMINATION (PED) SYSTEMS, 8 MAY 2013

i. DOD 8510.01: DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP), NOVEMBER 28

j. CENTCOM REGULATION 25-28: INFORMATION TECHNOLOGY INTRODUCTION AND PORTFOLIO MANAGEMENT, 7 SEPTEMBER 2012

k. NATIONAL INSTITUTE OF STANDARDS (NIST) SPECIAL PUBLICATION 800 SERIES

l. MIL-STD-498, MILITARY STANDARD: SOFTWARE DEVELOPMENT AND DOCUMENTATION (05 DEC 1994)

m. INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE) SYSTEMS ENGINEEERING BODY OF KNOWLEDGE

n. DEFENSE ACQUISITION GUIDEBOOK

o. PROJECT MANAGEMNT INSTITUTE (PMI) BODY OF KNOWLEDGE

p. FY91 NATIONAL DEFENSE AUTHORIZATION ACT SECT 1104

Appendix (C): Sample OEIS Measures of Performance and Effectiveness

OEIS Measures of Performance and Effectiveness for Counter Trafficking Airborne Detection and Monitoring

Effective systems engineering requires carefully scoped requirements captured in objective, testable, metrics together with targeted objective and threshold values for those metrics. Metrics should include Measures of Effectiveness (MOE) that come directly from operational user descriptions of critical use cases and desired outcomes. MOE should be tightly coupled to objective Measures of Performance (MOP) that describe critical measurable and testable aspects of systems and processes. Given MOE, MOP, and associated objective and threshold values, a chief engineer can objectively manage risk by devoting sufficient time, people, equipment and funds to execute a test strategy that iterates around requirements measured at key integration points.

MOE and MOP for Counter Trafficking Detection and Monitoring (D&M) capabilities have to do with finding, fixing, and engaging high value individuals (e.g. drug traffickers), events (e.g. drug transactions), and/or assets (e.g. drug caches). MOE and MOP for acquisition process will be around "speed-to-capability", i.e. the ability to rapidly intercept new technologies and apply them to rapidly evolving CONOPS and missions. Applying this general approach to the Afghanistan counter drug mission, representative Concept of Operations (CONOP) MOE, and MOP might be as follows:

Notional Mission-Level CONOPS:

Military and DEA agents plan daily operations based on commander's intent and current intelligence. This process identifies daily Courses of Action (COA) and Critical, Conditions of Interest (CCI). CCI are alert criteria for observable people, events, or things whose identification will result in changes in planned COA. For example, if a high value target is identified, all assets might be dynamically re-assigned to interdict that target.

Agents disperse in vehicles across area or responsibility (AOR) to execute their daily counter narcotics mission. The D&M aircraft flies its daily ISR mission aligned with highest priority collection requirements. J2/J3 analysts and watch standers collect and evaluate incoming intelligence. In the event that CCI are discovered while executing planned COA, agents and supporting J2/J3 assets respond accordingly to execute the emergent critical COA.

Engineering/Acquisition-Level CONOPS:

The Deputy Assistant Secretary of Defense for Counter Narcotics and Global Threats (DASD-NC) investment strategy aims to catalyze cross-department collaboration by incentivizing and enabling effective information collection and sharing among those

departments. Counter Narcotics and Global Threat information systems must support rapidly evolving missions, mission partners, areas of operations, and CONOPS. Further, these systems must be designed to intercept rapidly evolving technological tools. Hence, a modular, open, standard, architecture (MOSA), together with agile engineering and acquisition "plug-and-play" functionality, is key. In particular, systems designed and deployed to support one customer and mission must not only leverage the previously deployed capability, but also adapt to support future, as yet unknown, requirements.

Operational System-Level Metrics

MOE:

E1. Outcome (for finding): High Probability of Detection (Pd) of the critical drug trafficker(s), drug transaction(s), and/or drug source/cache of interest supports successful interdiction and legal prosecution.

> **Measure**: Percent improvement in modeled/simulated Pd compared to baseline value where, e.g., Pd = (Correct IDs ÷ Total Incidents) – (False Positives ÷ Total Incidents)
>
> **Objective**: Pd = 100%.
> **Threshold**: Pd improves with every delivery spiral.

E2. Outcome (for fixing): Fixed spatial and temporal location of critical individual, event, or asset is sufficiently accurate to support successful interdiction and legal prosecution.

> **Measure**: Horizontal coordinates, e.g., degrees and decimal degrees of latitude and longitude per WGS 84, and seconds and decimal seconds per UTC of critical person, event, or thing.
>
> **Threshold**: Surveilled object's horizontal position fixed at +/- 3m σ_{90} from airborne ISR platform. Ground mobile PED node horizontal position fixed at location fixed +/- 10m σ_{90}. Specifically prepared ISR artifacts meet criteria to serve as evidence in Court of Law
>
> **Objective**: Surveilled object's horizontal position fixed at +/- 1cm σ_{90} from airborne ISR platform. Ground mobile PED node horizontal position fixed at location fixed +/- 3m σ_{90}. All collected ISR artifacts meet criteria to serve as evidence in Court of Law

E3. Outcome (for engaging): Detect-to-decision time line is short enough to support successful interdiction, and subsequent prosecution, of critical targeted people, events, and things.

Measure: Minutes, and seconds between identification of CCI of and execution of associated decision to interdict
Threshold: 20 minutes. (The important consideration is that capability measurably improves over time as equipment and CONOPS improve.)
Objective: 10 minutes.

System Level MOP:

P1. Outcome: Critical Conditions of Interest CCI are identified. CCI are observable items of information that, if they change beyond identified threshold values, would cause decision makers to change the current course of action.

Measure: yes/no
Threshold: yes
Objective: yes

P2. Outcome: All ground nodes can cue/slew airborne sensors/PED in response to evolving CCI in near real-time

Measure: yes/no verified compliant with STANAG 4586 Interoperability Level 3; latency in seconds and decimal seconds
Threshold: yes; 1 sec
Objective: yes; 0.01 sec

P3. Outcome: GMTI radar cues FMV field of view to moving target of interest for ID and fixing

Measure: yes/no verified compliant with STANAG 4586 Interoperability Level 3
Objective: yes
Threshold: yes

P4. Outcome: distributed, deployed, DEA agents and DoD analysts share interactive Common Operating Picture (COP) in near real time

Measure: Tracks exist on shared COP yes/no; latency in decimal seconds
Threshold: yes; 1.0 second
Objective: yes; 0.01 second

P5. Outcome: Unambiguous and correctly identified tracks and contacts appear on COP along with notations

Measure: yes/no
Threshold: yes
Objective: yes

P6. Outcome: Each node can update COP with images, notations, contacts and/or tracks (as appropriate) and can interact via Internet Relay Chat.

Measure: yes/no
Threshold: yes
Objective: yes

P7. Outcome: Sensitivity of sensor plus Processing, Exploitation and Dissemination (PED) tools is sufficient to identify CCI from within aircraft mission profile.

Measure: CCI size plus probability of correct identifiable under mission parameters.
Threshold: Vehicle sized critical target correctly identified and tracked from mission flight level 80% of the time with false alarm rate no more than 20%
Objective: Human sized critical target correctly identified and tracked from mission flight level 80% of the time with false alarm rate no more than 20%

P8. Outcome: Beyond line of sight (BLOS) bandwidth supports sharing Full Motion Video usefully.

Measure: MBS per second
Threshold: 3 MBS
Objective: 5 MBS

P9. Outcome: Beyond line of sight (BLOS) range is sufficient to share COP, including FMV, across all relevant nodes.

Measure: Dimensions of operational area of interest
Threshold: Tactical Theater of Operations (Afghanistan)
Objective: Tactical plus Strategic Theater of operations (Global)

P10. Outcome: Critical message latency, including FMV, text, and image files supports successful interdiction of emergent targeted individual, event, or thing.

Measure: minutes, seconds, decimal seconds
Threshold: 5 sec
Objective: 1 Sec

P11. Outcome: Need-to-share policy is specified and implemented robustly. (Need-to-share policy is the basis for allowing or denying access to network data and resources. In that sense, need-to-share policy is the basis of IA/CDS risk analysis.)

Measure: yes/no

Threshold: yes
Objective: yes

P12. Outcome: Certified and Accredited Cross-domain Solution (CDS) implements dynamic need-to-share policy across security domains in order to support interdiction of emergent targeted person, event, or thing, i.e., in near real time.

Measure: Protection Level (PL) (equivalent); message latency in decimal seconds
Threshold: PL4 (equivalent); 1.0 second
Objective: PL5 (equivalent); 0.01 second

Engineering/Acquisition Process-Level Metrics

Process-Level MOE:

E4. Outcome: Continuously improving, cost-effective, capability.

Measure: Utility-per-Time-per-Cost where the measure of utility is MOE; measure of time is delivery schedule; and measure of cost is budget in dollars.
Threshold: Threshold MOE, delivered on schedule on budget
Objective: Objective MOE, delivered on schedule on budget

Process-Level MOP:

P13. Outcome: Capability modules, i.e. system components, include life cycle support, i.e. guaranteed tech refresh, at known cost.

Measure: yes @ cost in annual dollars; for some percent of required capability/no
Threshold: yes @ budget; for 70% of required capability
Objective: yes @ budget; for 90% of required capability

P14. Outcome: System components configure out-of-the-box.

Measure: time in months and weeks required to bundle, test, and certify capability component
Threshold: six months
Objective: three months

P15. Outcome: System components are readily consumable via convenient procurement vehicle and delivery mechanism

Measure: procurement lead-time in days, weeks, and months required to receive delivery of capability component

Threshold: one month
Objective: one week

P16. Outcome: New capability components that are developed at government expense (rather than procured off-the-shelf) include unlimited government rights to intellectual property, lifecycle support model, configure out-of-the-box, and are readily consumable via convenient procurement vehicle and delivery mechanism

Measure: General Purpose License (GPL) to developed capability exists yes/no; MOP per above going forward
Threshold: yes; per Threshold MOP above
Objective: yes; per Objective MOP above

Appendix (D): Sample OEIS Information Assurance (IA) Plan

Introduction

This document explains and details the plan for the Certification and Accreditation (C&A) of the PS-PEDS. The PS-PEDS is an Intel-based computer processing environment operating on the Windows platform which, when installed in a complimentary, and if necessary, certified host environment, provides for the manipulation of sensor systems, such as gimbal and mode control of an EO/IR sensor. In addition, the PS-PED can provide limited control, for example frequency and mode control, of properly configured co-located communication resources. Finally, a PS-PED mission requirement is to provide for the ingest and manipulation of sensor data, which can then be displayed, made into a digital or hard copy, or disseminated in near real time to a properly certified and configured system, via either a serial interface or a TCP/IP connection. Data is also available in the proper DCGS integrated Baseline (DIB) format so that products can also be distributed through a Unified Cross Domain Management Office (UCDMO) certified Cross Domain Solution (CDS). A CDS ancillary kit for the PS-PEDS is an available option and is separately certified and accredited.

Summary

The unique nature of the PS-PEDS makes addressing the C&A process timely and comprehensively critical. First, although it is a Department of Defense (DOD) funded and delivered effort, operationally the PS-PEDS will be deployed and maintained by the Drug Enforcement Agency (DEA) under the Department of Justice (DOJ). Secondly, although the first scheduled deployment is for Afghanistan, under CENTCOM, the PS-PEDS are intended to be deployable to and interoperate with multiple alternative sites. Finally, the PS-PEDS are intended to be operated as a tactical edge system, alternatively supporting Intelligence Sensor and Reconnaissance (ISR) missions for DOJ, DOD, or both. For these reasons, the approach to C&A should be comprehensive yet tailorable to meet mission requirements.

Conclusion

The plan for C&A of the PS-PEDS is to design and integrate it to meet the most stringent requirements, with the flexibility to relax any of the requirements when or if the system is deployed to environments where the more stringent requirements are not necessary. Additionally, by provisioning the CDS as an ancillary kit, it is possible to deploy a fully C&A'd PS-PED in environments where there is no CDS required for much less time and cost than if the systems were bundled together. The PS-PEDS will be developed and implemented to meet the full requirements of a Mission Assurance Category (MAC) II system with a Level of Confidentiality (LOC) of Sensitive, but Unclassified (SBU) under the DIACAP. Meeting this requirement provisions the most stringent of the DOD environments to which the system can be deployed. In addition, because there are specific provisions for law enforcement that are not totally covered by the DIACAP, the additional DOJ NIST SP 800-53 requirements will be identified, addressed, and either met by the DIACAP requirements or added, as required. Finally, because of the deployment to the CENTCOM Theater of operations, those requirements of 25-28 will also be met. In the event the C&A authority determines that some of these assurance controls are not necessary, they can be relaxed as deemed responsible, but the PS-PEDS will be developed and integrated to meet them all.

Detailed Description

This section provides details of the analysis to support the conclusion above. The primary goal of the C&A is to achieve and maintain an Authority to Operate (ATO). Ordinarily this is accomplished through a process of test and evaluation of the system, usually called Certification Test and Evaluation (CT&E or CTE). In this step, the evidence of the assurance of the system is evaluated by authorized evaluators, the risks identified are confirmed, and the mitigations validated. The evidence required is provided by the system integrator in the form of demonstrations and deliverables. Upon successful completion of this step, the system is typically provided with an Interim Authority to Operate (IATO). The IATO is used to test the system, a process often called Security Test and Evaluation (STE).

STE is typically a period of three or four weeks, whereupon the system is issued an ATO. The ATO must be maintained, most often by updating the evidence and configuration annually. At some time, the ATO may need to be renewed. Upon completion of the use of the system, the ATO and the system are both retired.

Basis for Decision

In an effort to facilitate reciprocity, as well as ease the burden for C&A, security controls identified in NIST SP 800-53 have come to be used more commonly. For DOD systems, this process is embodied in DODI 8510.01a, the DIACAP. Almost all DOD IS systems that connect or operate go through some version of the DIACAP because it is the most comprehensive process normally used. It is worth noting that one of the first steps in the DIACAP was to change the name of the DSAWG from the DISN Security Accreditation Working Group to the Defense Security Accreditation Working Group, thereby indicating the increase in the span of concern for vulnerabilities in IS systems. The DIACAP process is well documented and understood. In addition to the controls provided through the DIACAP, systems may be C&A'd via other processes. In particular, DOJ systems are usually done through the NIST SP 800-53, which is, for the most part, the parent document of the DIACAP. The DOJ requirements for the system are concerned primarily with the use of the results as evidence in legal cases and the protection of any personal privacy information. In recent years, with the increased use of IS systems in record keeping various laws have been passed protecting personal information, such as social security numbers, health information, bank information, and so forth. For the most part, DOD security controls, such as those in the DIACAP, are not concerned with this type of personal information; rather they are aimed at protecting national security information. Therefore, in order to comply with the DIACAP DOD requirements and assure that we still meet any additional DOJ requirements, we will meet the normal controls for the DIACAP and evaluate the need to add any additional specific controls from the NIST SP 800-53. In the course of the evaluation, we will determine if we have already met some or all of the control

requirements through the DIACAP process. Where we have not, we will supplement the additional controls as required. In every case, we will document how we have met the additional DOJ controls. This entire body of evidence will then be presented to the Decision Accreditation Authority (DAA) for an IATO. Once the IATO is achieved, the C&A will be coordinated through the DOJ CIOs office for any additional DOJ permissions required. Once achieved, the ATO will then be maintained as required on an annual basis until the system is retired.

System Constraints

In order to meet the operational needs of the ISR system, we have evaluated it at Mission Assurance Category (MAC) II, with a Level of Confidentiality (LOC) of Unclassified (U). Thus, there is no provision to operate the system at a classified level. There is a separate option in the PS-PEDS for a CDS, and when exercised, the C&A for the CDS would be accomplished as required, through the use of a Cross Domain Appendix (CDA) via the UCDMO. In this case, however, the PS-PEDS would interface to a classified system, which is already provisioned through some other means and has already achieved an ATO. The PS-PEDS would not seek to obtain an ATO for a classified system nor would it deploy or operate one. If one was available, and the CDS option was exercised, then the PDS-PEDS would be capable of interfacing to it and making data available to it. Any of the data available in the closed ISR network could also be passed through the ancillary CDS.

Security Controls

For virtually all DOD systems which connect, security controls are identified through the DIACAP process, which is based on NIST SP 800-53. Intelligence system controls, of which ISR systems are frequently a part, are ordinarily identified through the Intelligence Community Note (ICD) 503, which is based on the CNSSI 1253. Since this is a recent requirement, many intelligence systems are still being certified through the older process, based on the DCID 6/3. In either case, these systems normally can interoperate DOD systems with little or no additional C&A. Historically, however, ISR systems are usually Top Secret with caveats, and hence a CDS must be used, which requires a separate C&A. In the case of Global Discovery,

as well as in the case of numerous Persistent Intelligence Surveillance Reconnaissance (PISR) systems, where the results must be shared with coalition and cooperating participants, including foreign government agencies, first responders, and even NGHOs, C&A does not fall under the ICD 503 requirements. Therefore, in most cases, it is being addressed, for DOD requirements, through the DIACAP process. Because of the use of the data collects for the GD ISR system, the data cannot be classified, since it is expected to be used in open court, including in some cases foreign courts, as evidence. Additionally, some of the data collected and used may fall under certain Personal Privacy Information (PPI) restrictions. There are a variety of these, each related to the specific type of information, such as social security information, criminal records, banking information, housing information, telephone numbers, health information, and so on. As a result, the Drug Enforcement Agency (DEA), which does not use the DIACAP process, has controls which are derived from the NIST SP 800-53. Since this is the parent document for the DIACAP controls, we anticipate that blending the two sets of the controls for the PS-PEDS will be simple. Thus, the overall strategy is to use the DIASCAP controls for MAC II, LOC U, which the required availability, and identify these through the DIACAP process creating a standard DIACAP Scorecard. Then the separate controls from the NIST SP 800-53 will be added, as identified, to the scorecard. Where any of the controls have already, due to the DIACAP process, been identified, they will be noted as meeting both DOD and DEA requirements. This then will be used to identify the evidence package which must be created for the C&A. Additionally, we will determine the proper DOD required PPSs, STIGs, and run the scans for the host system and establish these as early as possible as part of our test and integration system. These will be configuration controlled and maintained throughout the test and integration phase and will be delivered as part of the production system. Because the PS-PEDS and the GD-aircraft are separately procured and delivered systems, a separate C&A package, also under the DIACAP, for MAC II, LOC U, will be developed for that system.

Early Involvement of the Decision Accreditation Authority (DAA)

In every case of C&A, liaison with the DAA for the system yields the best results. For the PS-PEDS, with the compressed timeline, it is considered critical. Therefore, as soon as the System Identification Profile (SIP) for both the PS-PEDS and the GD-aircraft have been signed, and the requirements validated, we will begin working with the identified DAA to refine and tailor the C&A package, as identified above, for actual deployment and operation. By putting the package together as identified above, we believe that the system can be C&A'd at a sufficiently complete level so that it can be deployed to any theater where DOD and DEA operate. As currently identified, it is scheduled to be deployed to CENTCOM. The CENTCOM Theater has specific requirements as identified in CCR 25-28. For this specific deployment, we will, after assembling the evidence package as discussed above, tailor it specifically to meet the CCR 25-28 requirements. It is expected that through this process, we will also meet the Joint Interoperability Test Command (JITC) interoperability requirements, as required by CJSCI 6212.01F.